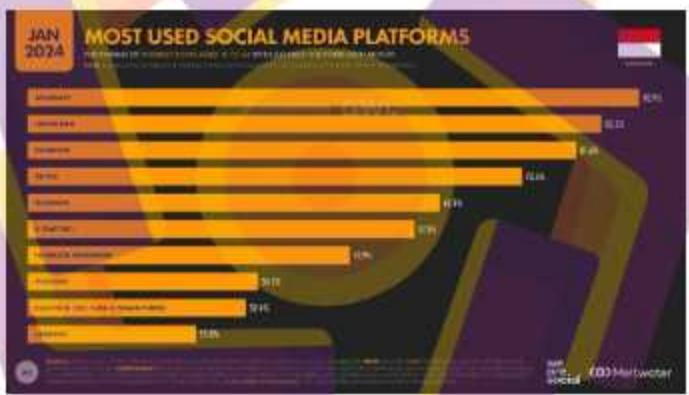
BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era industri 4.0 yang terus berkembang, terdapat berbagai aplikasi media sosial yang beredar di masyarakat. Jumlah pengguna aktif media sosial mengalami peningkatan yang signifikan. Salah satu platform media sosial yang paling banyak digunakan adalah WhatsApp [1]. Melalui penggunaan media sosial, pengguna dapat melakukan berbagai aktivitas, seperti mengunggah gambar, video, dan cerita singkat. Selain itu, para pengguna media sosial juga memiliki kemampuan untuk berinteraksi dengan pengguna lainnya melalui komentar, memberikan "like" pada postingan, serta melakukan repost terhadap konten yang menarik.



Gambar 1. 1 platform media sosial yang sering digunakan [2]

Media sosial merupakan alat yang kaya fitur, menawarkan kemampuan untuk terhubung dengan orang lain, mencari teman, dan berinteraksi melalui berbagai konten. Seiring dengan meningkatnya jumlah pengguna internet, data yang tersedia di platform-platform ini juga semakin melimpah. Informasi yang bersifat open source dapat diakses dengan mudah, dan Open Source Intelligence (OSINT) berfungsi untuk mengumpulkan serta menganalisis data tersebut dari berbagai sumber, termasuk media sosial dan blog [3].

Media sosial, dengan berbagai kemampuannya, telah menjadi alat yang kaya fitur untuk berkomunikasi dan berinteraksi. Seiring dengan meningkatnya jumlah pengguna internet, volume data yang tersedia di platform-platform media sosial juga semakin besar. Informasi yang tersebar di berbagai platform ini sering kali bersifat open source, yang artinya dapat diakses secara terbuka oleh siapa saja. Open Source Intelligence (OSINT) merupakan metode untuk mengumpulkan dan menganalisis informasi yang diperoleh dari sumber terbuka tersebut, termasuk dari media sosial, blog, dan berbagai situs internet lainnya. OSINT memiliki peran yang sangat penting dalam memanfaatkan data yang ada untuk tujuan analisis dan pengambilan keputusan, baik dalam konteks keamanan siber, investigasi, maupun intelijen.

Namun, meskipun banyak informasi yang dibagikan di media sosial dapat memberikan manfaat, terdapat juga risiko besar terkait dengan kebocoran data pribadi. Banyak pengguna media sosial yang tanpa sadar membagikan informasi sensitif, seperti alamat rumah, tanggal lahir, nomor telepon, dan jenis kelamin. Informasi ini, yang terkadang dapat diakses oleh publik, berpotensi disalahgunakan oleh pihak-pihak dengan niat jahat, seperti untuk merencanakan kejahatan atau tindakan teroris. Oleh karena itu, pemahaman yang lebih dalam tentang potensi ancaman yang ada pada media sosial dan bagaimana cara mengidentifikasinya melalui OSINT sangatlah penting.

Das (2008), membuat lima instrumen utama dengan bantuan akal dalam memperoleh informasi, yaitu (1) akal manusia (HUMINT), mengumpulkan informasi melalui kontak manusia, seringkali berupa informasi tentang nama, lokasi, waktu, gerakan target dan niat target; (2) Signal Intelligence (SIGINT) adalah kumpulan informasi dari satu titik kontak. Radiasi elektromagnetik (pemisahan), secara umum, dari perangkat elektronik; (3) Ilustrasi Intelijen (IMINT) adalah kumpulan informasi dari sumber. [4] Setiap orang melakukan OSINT memiliki alasan dan tujuan tertentu, misalnya hanya ingin berkenalan, stalker, mencuri dokumen, doxing, kegiatan hacking, mencuri dokumen, dan lain lain. Peran Open Source Intelligence (OSINT) dalam mendeteksi Gerakan Kelompok Separatis Teroris (KST) yaitu :

1. Ethical Hacking dan *Penetration Testing*

Professional keamanan menggunakan open source intelligence untuk mengidentifikasi potensi kerentanan dalam jaringan sehingga dapat diperbaiki sebelum dieksploitasi oleh peretas. Kerentanan yang sering ditemukan antara lain : kebocoran informasi sensitif yang tidak disengaja, seperti melalui media sosial, perangkat yang tidak di patch, seperti situs web yang menjalankan produk CMS umum versi lama dan aset yang bocor atau terbuka, seperti kepemilikan kode pada pastebin.

2. Identifikasi Ancaman Eksternal

Internet memberikan informasi yang sangat baik tentang ancaman yang paling potensial bagi perusahaan. Berawal dari menemukan kerentanan baru yang bisa disalahgunakan secara aktif hingga mengintersep obrolan penyerang tentang serangan yang akan datang. Terdapat banyak kasus, jenis pekerjaan ini mewajibkan untuk melakukan analisis, mengidentifikasi, dan menghubungkan

3. Mengungkap Strategi Sisi Gelap dalam Kejahatan Terorisme Melalui OSINT

Banyak bisnis kecil dan menengah didirikan setiap tahun karena proses ini. Ini tidak terjadi karena kelompok peretas sangat tertarik pada mereka. sebaliknya, ini terjadi karena kesalahan yang ditemukan dalam arsitektur jaringan atau situs web mereka yang dibuat dengan teknik open source intelligence sederhana. Meskipun kecil kemungkinan seorang teroris akan memposting lokasi target pilihannya secara online, langkah-langkah ini membantu memantau pandangan ekstremis kekerasan. kami berpendapat bahwa mengumpulkan Informasi Open Source adalah alat yang sah untuk tata kelola keamanan (Hayes, 2010). Namun, meningkatnya legitimasi penggunaan OSINT tidak dapat diperoleh semata-mata dari mengejar masalah keamanan atau keselamatan [5]

1.2 Rumusan Masalah

Berdasarkan paparan latar belakang diatas, rumusan masalah dalam penelitian ini yaitu :

1. Tools apa saja yang bisa digunakan untuk OSINT
2. Informasi apa saja yang bisa diperoleh menggunakan teknik Digital Footprinting dan OSINT
3. Batasan data pribadi yang boleh disertakan dalam media sosial

1.3 Batasan Masalah

Agar penelitian ini lebih terarah dan sesuai dengan rumusan masalah yang telah dipaparkan sebelumnya, peneliti membuat batasan masalah. Batasan masalah yang ditetapkan dalam penelitian ini adalah sebagai berikut:

1. Pelaksanaan penelitian ini untuk menganalisis keamanan profil media social Instagram Desy Ikasari https://www.instagram.com/desykaaaaaa/ dan Instagram Djon afriandi https://www.instagram.com/djonafriandi/
2. Peneliti melakukan *Digital footprinting* untuk mendapatkan data yang dibutuhkan
3. Mengumpulkan data menggunakan metode dorking, Mengunakan Tools Open Source
4. Validasi Data Menggunakan Tools khusus Osint Dan Web Open Source

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mencari data apa saja yang bisa didapat menggunakan metode OSINT Dan Edukasi seberapa berbahaya efek dari kebocoran data.

1.5 Sistematika Penulisan

Sistematika penulisan berisikan garis besar atau gambaran secara umum penelitian ini sehingga mempermudah pemahaman alur isi. Adapun garis besar isi skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN, tahapan ini merupakan bab awal yang menjelaskan tentang latar belakang , masalah penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penyajian.

BAb II LANDASAN TEORI, bab ini menjelaskan tinjauan kepustakaan dari penelitian-penelitian terkait yang membahas beberapa teori antara lain apa itu OSINT, teknik OSINT (dorking, profiling media sosial, footprinting)

BAB III METODE PENELITIAN, bab ini berisikan gambaran umum tentang alur dari penelitian, prosedur, dan mekanisme metode analisis yang diterapkan pada penelitian.

BAB IV HASIL DAN PEMBAHASAN, bab ini merupakan tahapan yang penulis lakukan dalam mengembangkan aplikasi, testing hingga penerapan aplikasi di objek

penelitian,

BAB V PENUTUP, berisi kesimpulan dan saran yang dapat peneliti rangkum